Security Smart

Incidents of Security Concern

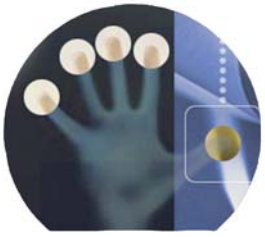
Fortunately, the majority of LANL workers have no experience with "security incidents". And for those who do, personal cell phone incidents are typically the extent of their involvement. This Security Smart provides the LANL worker basic information about Incidents of Security Concern (IOSCs), and how they are addressed.

The Security Inquiry Team (SIT) is the sole LANL entity that evaluates and categorizes potential security incidents and conducts inquiries into IOSCs per the Department of Energy (DOE). The SIT provides managers and workers information necessary to evaluate operations toward the goal of eliminating security incidents and thereby protecting the vital work done at the Lab.

The Security Inquiry Team is comprised of approximately 10 Los Alamos Site Office (LASO)-appointed Inquiry Officials (IOs) with extensive backgrounds in a variety of LANL disciplines. These IOs are augmented by a cadre of experienced IOs currently assigned to other LANL organizations and who are available to assist the SIT in the event of a major security inquiry. The SIT also routinely calls upon the expertise of various LANL scientific offices for assistance.

The SIT receives about 450 calls a year, of which about 175 are determined to be IOSCs, categorized as Impact Measurement Index (IMI)* 1-4. Matters that do not rise to the threshold of IOSC are categorized as *Security Events*. Both Security Events and IOSCs are captured in the SIT database, which supports extensive and routine analyses. Security Events are documented by the SIT on Security Call Assessment Records (SCARs), which are forwarded, usually within one or two days, to the affected organization for action. The SIT takes no further action on Security Events, and security infractions are not issued for Security Events.

Official inquiries are conducted by IOs on all IOSCs. Inquiries culminate in the issuance of a Report of Security Incident/Infraction, which details the inquiry process/results and concludes with a recommendation to Security Division (SEC-DO) for or against the issuance of a security infraction. SEC-DO is the authority designated to issue LANL infractions. The percentage of security infractions issued continues to drop as LASO has allowed SEC-DO to increasingly consider extenuating circumstances when making the infraction determination. The Inquiry Report is provided to the affected LANL division for causal analysis and corrective actions. The SIT maintains the official file on the incident, including the inquiry report, supporting documentation, causal analysis, and corrective actions.



Impact Measurement Index*

IOSCs are categorized based on DOE's IMI tables. The IMI roughly reflects an assessment of an incident's potential to (1) cause serious damage to national, DOE, or LANL security, operations, resources, or workers or (2) degrade or place at risk safeguards and security interests or operations. Four categories of security incidents have been established based

Reference: DOE Manual 470.4-1, Section N, *Categories of Incidents of Security Concern*

on the relative severity of the incident. The IMI categories range from IMI-1 (most severe) to IMI-4 (least severe). Each of these four categories is further subdivided into specific categories.

Impact Measurement Index

Categories of Incidents of Security Concerns (DOE M 470.4-1, Section N)

IMI-1	Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public. IMI-1 includes, but is not limited to, (1) confirmed or suspected loss, theft, or diversion of a nuclear device or components or weapon data; (2) confirmed or suspected intrusions, hackings, or break-ins into DOE computer systems containing Top Secret, SAP information, or Secret Compartmented information; and (3) confirmed or suspected acts or attempts of terrorist actions.
IMI-2	Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. IMI-2 includes, but is not limited to, (1) any amount of special nuclear material found in a dangerous or hazardous unapproved storage environment or unapproved mode of transportation or transfer; (2) confirmed or suspected unauthorized disclosure, loss or potential loss of Secret matter; and (3) confirmed compromise of root/administrator privileges in DOE unclassified computer systems.
IMI-3	Action, inactions, or events that pose threats to DOE security interest or that potentially degrade the overall effectiveness of DOE's safeguards and security protection programs. IMI-3 includes, but is not limited to, (1) confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter; (2) actual or attempted introduction of controlled/prohibited articles, except cell phones and personal digital assistants (PDAs), into a security area; and (3) demonstrators or protestors that cause site and facility damage.
IMI-4	Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE safeguards and security interests. IMI-4 includes, but is not limited to, (1) confirmed or suspected unauthorized disclosure of Unclassified Controlled Nuclear Information (UCNI); (2) actual or attempted introduction of unauthorized cell phones or PDAs into a security area; and (3) failure to adhere to established administrative procedures pertaining to foreign nationals.

Immediate Reporting

One of the SIT's most important responsibilities is to respond immediately to potential IOSCs and assist affected organizations in rapidly identifying and mitigating vulnerabilities. In so doing, many IMI-1s can be mitigated to IMI-4s — and infractions possibly avoided. But timely response is predicated on immediate reporting to the SIT. General Security ISD 201.1, Part 3, requires all LANL workers to immediately report to the SIT and their security-responsible line managers (SRLMs) any *potential* IOSC.

Incident Initiatives

The SIT and Security Division are continually working to shift the emphasis of IOSC from reporting incidents to eliminating them. This reduction can be accomplished by immediate reporting of potential incidents to the SIT and thorough causal analyses and corrective actions. Additionally, SEC-DO has advocated an overhaul of the IMI due to ambiguity and inconsistencies in interpretation. For the time being, however, the IMI is used throughout the DOE complex; hence Laboratory employees must understand the types of actions that fall under the IMI categories.

Resources: Security Inquiry Team (5-3505) and Security Help Desk (5-2002)